Department of Homeland Security Daily Open Source Infrastructure Report for 14 June 2006

Current Nationwide Threat Level is ELEVATED — Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Department of Energy says that last September, a hacker stole a file containing the names and Social Security numbers of 1,500 people working for the Department's National Nuclear Security Administration in Albuquerque, New Mexico. (See item 12)
- The Departments of Homeland Security and Transportation have released an assessment of mass evacuation plans for catastrophic hurricanes and other such events impacting the Gulf Coast region. (See item 30)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *June 13, Reuters* — **U.S. governors adopt energy plans for the West.** Governors of states in the U.S. West approved proposals over the weekend to add cleaner energy resources to meet the region's growing demand for electricity. The Western Governors Association, which represents 19 states and three U.S.−flag islands in the Pacific, passed measures that call for 30,000 new megawatts of clean energy supplies such as solar and geothermal power by 2015. The Western governors also called on the U.S. Federal Energy Regulatory Commission to work with the states to make the regional power grid more efficient and to expand it to tap renewable energy supplies in remote areas.

Source: http://abcnews.go.com/Technology/print?id=2068060

2. *June 12, Reuters* — **U.S. sees no cut in Iraq oil attacks after Zarqawi.** The U.S. is not expecting a decrease in attacks on Iraq's oil infrastructure in the short term after the death of al Qaeda's Iraq group leader Abu Musab al−Zarqawi, U.S. Department of Energy Secretary Sam Bodman said on Monday, June 12. Bodman pointed out that attacks from the insurgency on pipelines and oil export facilities were still occurring in Iraq. "I would expect that would continue at least for a while," he said. Iraq's crude oil production in May was 1.9 million barrels a day, down sharply from almost 2.6 million barrels a day in January 2003, just before the start of the U.S.−led invasion of Iraq, according to the U.S. Energy Department. Iraq is the sixth biggest foreign oil supplier to the United States.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/06/12/AR2006061200686.html

3. *June 12, Reuters* — **Explorer shuts products pipeline on Oklahoma tank fire.** Explorer Pipeline Co. said Monday, June 12, it has shut its 28−inch oil products pipeline into Tulsa, OK, and the 24−inch pipeline out of Tulsa to Wood River, Illinois, because of a products tank fire in Glenpool, Oklahoma. As of Monday morning, June 12, the tank fire had not damaged the pipeline but Explorer will wait for the fire to be put out before deciding when to reopen it, Rod Woodford of Explorer, said. Woodford said some local pipelines in the Explorer system were running. Explorer operates a 1,400−mile pipeline system that transports gasoline, diesel fuel, and jet fuel from the Gulf Coast to the Midwest. Captain Larry Bowels of the Tulsa Fire Department said the fire started at 9 a.m. CDT. Bowels said the fire was still burning and that the tank was a fixed−roof, 150,000−barrel unleaded gasoline tank and that the fire was confined to that tank. The Explorer Website says that via connections with other products pipelines, Explorer serves more than 70 major population centers in 16 states.
Source: http://biz.yahoo.com/rb/060612/energy_explorer_fire.html?.v=1

4. *June 12, Charlotte Observer (NC)* — **Powerful storm in Southeast knocks out power.** Power was out through Monday morning, June 12, to nearly 10,000 customers in the Charlotte metro region after powerful thunderstorms swept across the area Sunday afternoon and evening. No serious injuries were reported, but damage was widespread. The weekend storms formed in conditions that produced the hottest weather so far this year. Temperatures in Charlotte climbed to 94 degrees both on Saturday and Sunday −− and heavy storms formed each day. At the peak of damage Sunday evening, more than 65,000 Duke Energy customers were without power. Thousands of customers from other electric companies also were in the dark from the storms, which were especially bad in Mecklenburg, Gaston, Rowan, and Davie counties. The Charlotte Fire Department said it received more than 200 calls for help Sunday, including more than 30 calls about downed power lines.
Source: http://www.centredaily.com/mld/centredaily/news/nation/14797492.htm

5. *June 09, Associated Press* — **Railroads struggle to ship coal in U.S.** Power plants around the country have seen their coal stockpiles dwindle, mainly because of problems with shipping coal out of Wyoming and increasing worldwide demand for energy. The two main shippers of U.S. coal −− BNSF Railway Co. and Union Pacific (UP) Railroad −− say they are investing hundreds of millions of dollars in order to ship more Wyoming coal and keep up with an ever growing demand for power. Transportation analyst Anthony Hatch said he believes railroads

will meet future demands for shipping coal. But it will take time because of the enormous task of expanding an industry that until only a few years ago was abandoning track as its business dwindled. But until the rail system can match rail capacity and demand for service, there will be periods where rail shipments can't keep up, he said. BNSF and UP are investing $200 million in an expansion project, which they expect to be able to ship more than 400 million tons of coal a year. The Dakota, Minnesota & Eastern Railroad is seeking $2.5 billion in federal loans to extend and rebuild rail lines so it can haul Wyoming coal to the Midwest and Great Lakes regions.
Source: http://www.chron.com/disp/story.mpl/ap/business/3955144.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

6. *June 13, Associated Press* — **Two presumed dead in explosion at Iowa Army Ammunition Plant.** Two workers at an Army ammunition plant in Middletown, IA, are presumed dead after an explosion occurred Monday morning, June 12, officials said. The blast at the Iowa Army Ammunition Plant caused damage concentrated around a collapsed bay near one of the plant's five production lines. Two workers are missing and presumed dead; two others received minor injuries, according to a statement from American Ordnance, the ammunition manufacturer that runs the plant.
Source: http://www.wcfcourier.com/articles/2006/06/13/news/breaking_news/doc448e7f03b7884276289237.txt

7. *June 13, KNSD−TV (CA)* — **Chemical spill jams interstate in California.** Thousands of North County, CA, commuters found themselves trapped on the freeway Tuesday, June 13, after authorities shut down northbound Interstate 5 just north of Oceanside because of a toxic chemical spill. The traffic nightmare started when a car crashed into a pickup carrying swimming pool cleaning supplies just south of Las Pulgas Road. The truck overturned, spilling several gallons of muriatic acid and chlorine tablets. When the two chemicals mixed, a cloud of chlorine gas formed on the freeway.
Source: http://www.msnbc.msn.com/id/13299877/

8. *June 12, Associated Press* — **Authorities investigate central Illinois gasoline leak.** Authorities on Monday, June 12, were investigating the cause of a gasoline leak at the Buckeye Partners LP petroleum terminal in central Illinois that spilled about 71,000 gallons of fuel. No injuries were reported, and only one family that lived near the site just west of Harristown was evacuated from their home.
Source: http://www.belleville.com/mld/belleville/news/politics/14803 219.htm

[Return to top]

Defense Industrial Base Sector

9. *June 13, Reuters* — **U.S. insists on right to develop arms for outer space.** The United States on Tuesday, June 13, reasserted its right to develop weapons for use in outer space to protect its

military and commercial satellites and ruled out any global negotiations on a new treaty to limit them. In a speech to the Conference on Disarmament, a senior U.S. State Department arms control official insisted that such weapons systems would be purely defensive. John Mohanco, deputy director of the office of multilateral, nuclear and security affairs, said: "As long as the potential for such attacks remains, our government will continue to consider the possible role that space−related weapons may play in protecting our assets." The White House is due to announce a new space policy this month, the first overhaul in a decade.
Source: http://www.defensenews.com/story.php?F=1867998&C=america

10. *June 12, Society Of British Aerospace Companies* — **UK defense industry anti−corruption forum.** The UK's leading defense companies and defense sector Trade Associations have joined forces to set up the UK Defense Industry Anti−Corruption Forum. Representatives from 11 companies and two Trade Associations met on May 18 for the inaugural meeting of the Forum. The creation of the UK Defense Industry Anti−Corruption Forum reflects the shared determination of the key industrial partners to promote the prevention of bribery and corruption in the international defense market. All the participants in the inaugural meeting of the Forum have established policies in place that meet high ethical values, backed up with compliance procedures to ensure that their employees observe the laws in all the countries in which they operate. Their aspiration is that the Forum will help build on those policies and practices to ensure universally high standards in the global market.
Source: http://www.sbac.co.uk/community/cms/content/preview/news_ite m_view.asp?i=10684

[Return to top]

Banking and Finance Sector

11. *June 13, Reuters (UK)* — **Security breaches rise at financial firms.** More than three−quarters of the world's biggest banks and financial firms suffered an external security attack in the past year and half experienced an internal breach, the 2006 Global Security Survey from advisory firm Deloitte said Tuesday, June 13. Approximately 78 percent of big financial institutions reported a security breach from outside the organization in the past year, up from 26 percent the previous year. More than half of the external attacks were attributed to phishing and pharming. Mike Maddison of Deloitte said the scale and nature of the problem indicated a more serious threat had emerged. The survey of senior security officers at the world's top 100 financial firms said 49 percent of the institutions had experienced at least one internal breach of security in the last year, up from 35 percent a year earlier. Insider fraud and leakage of customer data were cited as the most common internal breaches.
Source: http://today.reuters.co.uk/news/newsArticle.aspx?type=fundsN ews&storyID=2006−06−13T061953Z_01_NOA322689_RTRUKOC_0_FINANC IAL−SECURITY−SURVEY.xml

12. *June 13, Associated Press* — **National Nuclear Security Administration computers hacked; Info on 1,500 taken.** Last September, a hacker stole a file containing the names and Social Security numbers of 1,500 people working for the Department of Energy's (DOE) National Nuclear Security Administration (NNSA). The data theft occurred in a computer system at a service center belonging to the NNSA in Albuquerque, NM. NNSA Administrator Linton Brooks said that he learned of the security breach late last September, but did not inform

Energy Secretary Samuel Bodman about it. NNSA said he assumed DOE's counterintelligence office would have briefed senior DOE officials. Brooks said the file contained names, Social Security numbers, date−of−birth information, a code where the employees worked, and codes showing their security clearances. A majority of the individuals worked for contractors and the list was compiled as part of their security clearance processing, he said. Tom Pyke, DOE's official charged with cyber security, said he learned of the incident only a few days ago. He said the hacker, who obtained the data file, penetrated a number of security safeguards in obtaining access to the system.
Source: http://www.forbes.com/entrepreneurs/feeds/ap/2006/06/12/ap28 10729.html

13. *June 13, Reuters* — **Japan's KDDI says customer data leaked.** KDDI Corp., Japan's second−largest telecoms operator, said on Tuesday, June 13, that personal information on nearly four million customers of its Internet service had been leaked. KDDI said information on subscribers to its Dion Internet access service as of December 18, 2003 was leaked to a third party including email addresses, phone numbers, gender, and birthdates. No credit or bank account data were leaked, it said. KDDI said it became aware of the leak on May 30 this year when a person called one its offices saying that he or she had obtained client data. The following day a CD−ROM with information on 400,000 customers was delivered to KDDI's headquarters. KDDI said it then entered into negotiations with the party holding the data and was able to retrieve all of the leaked information on Thursday, June 8.
Source: http://www.techweb.com/wire/security/189400574;jsessionid=D2KEFJ4KW5FWAQSNDLRSKH0CJUNN2JVN

14. *June 13, U.S. Department of the Treasury* — **Treasury identifies international financial network of Colombia's notorious North Valle drug cartel.** The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) on Tuesday, June 13, added five individuals and twenty companies tied to Colombia's North Valle drug cartel to its list of Specially Designated Narcotics Traffickers (SDNTs). The five individuals act as front persons for North Valle cartel leaders Raul Alberto Grajales Lemos (Raul Grajales) and Carlos Alberto Renteria Mantilla (Beto Renteria). Barbara Hammerle, Acting Director of OFAC, said "Today's action exposes a key financial network of the North Valle cartel...This network utilizes front companies in Colombia, the United States, Panama, and the British Virgin Islands to move its illicit proceeds. By exposing the financial backbone of Colombian drug cartels through our designation process, we thwart their ability to launder illicit proceeds." Also named are 20 companies which comprise an international financial network for Colombia's North Valle cartel. The 20 companies encompass a wide range of services including real estate, investment, construction, property management, and manufacturing. These entities are shell companies used to facilitate financial transactions. The 487 SDNT businesses include agricultural, aviation, consulting, construction, distribution, financial, horse breeding, investment, manufacturing, maritime, mining, offshore, industrial paper, pharmaceutical, real estate, and service firms.
Source: http://www.treasury.gov/press/releases/js4318.htm

15. *June 10, Websense Security Labs* — **Phishing Alert: Banque Nationale Du Canada.** Websense Security Labs has received reports of a new phishing attack that targets customers of Banque Nationale Du Canada. Users receive a spoofed e−mail message, which explains that a security audit has detected an unexplained transaction on their statement. Users are advised to review their statements and are provided with a link to a phishing Website that prompts them to

enter account information, such as username and password.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =516

[Return to top]

Transportation and Border Security Sector

16. *June 13, Associated Press* — **Southwest Airlines adds more flights in New Orleans.** Southwest Airlines has added six daily non−stop flights from New Orleans' Louis Armstrong International Airport, reclaiming the spot as the largest carrier operating from the area. Southwest was the airport's largest carrier before Hurricane Katrina virtually forced the airport to rebuild service from the ground up. The new flights bring Southwest's total to 24. While that's more than other carriers, it still amounts to only 43 percent of the of the airline's pre−Katrina service.
Source: http://www.usatoday.com/travel/flights/2006−06−13−southwest− new−orleans_x.htm

17. *June 13, Hamilton Spectator (Canada)* — **Airline suspends four mechanics.** Air Canada Jazz has suspended four mechanics a day after they publicly raised concerns about safety at the airline. Dave Avella, Gianni Ballestrin, Grant Anastas, and Ron Anstey, all mechanics at Jazz' Toronto facility, were suspended with pay pending an investigation by the airline into comments they made, including allegations that they are pressured to release planes with defects that could compromise public safety. Meanwhile, Transport Canada on Monday, June 12, said it was launching an audit into Jazz's mechanical operations in the next three months. Lucy Vignola, a spokesperson for the regulator, said inspectors will examine the airline's mechanical standards for compliance with federal regulations. Several Jazz mechanics who spoke with reporters, including the four who spoke publicly, say they've lodged complaints with Transport Canada inspectors about conditions at Jazz without response. The comments of the four mechanics included allegations that they are forced to cut corners in order to avoid costly delays in flight schedules, that some mechanical procedures are done in breach of regulations, and that there's a poor level of training and scrutiny over mechanical repairs at the airline.
Source: http://www.hamiltonspectator.com/NASApp/cs/ContentServer?pagename=hamilton/Layout/Article_Type1&c=Article&cid=1150149011021&call_pageid=1020420665036&col=1112101662670

18. *June 12, Pittsburgh Post−Gazette* — **Plane makes emergency landing in Pittsburgh.** A plane traveling from Washington Reagan National Airport to Lambert−St. Louis International Airport made an emergency stop at Pittsburgh International Airport on Monday, June 12, after one of its two hydraulic systems failed in the air. A backup system allowed the pilot to land AmericanConnection flight 5526 without injury to the plane's 38 passengers and three crewmembers. But after the regional jet landed, its backup system failed, too, forcing the St. Louis−based airline to tow its aircraft to the gate using a tug. The plane is operated by AmericanConnection, a regional affiliate of American Airlines and a unit of St. Louis−based Trans States Airlines Inc.
Source: http://www.post−gazette.com/pg/06163/697673−100.stm

19. *May 26, Government Accountability Office* — **GAO−06−475: Aviation Security: Further Study of Safety and Effectiveness and Better Management Controls Needed If Air Carriers Resume Interest in Deploying Less−than−Lethal Weapons (Report).** The Transportation Security Administration (TSA) has authority to approve air carrier requests to deploy less−than−lethal weapons, including electric stun devices, onboard commercial aircraft to thwart an attack. Since the terrorist attacks of 2001, one air carrier received approval to deploy electric stun devices. To address concerns regarding reports of injuries after the use of these devices and to ensure that the impacts of these devices onboard aircraft have been fully evaluated, this report answers the following: (1) What analyses has the federal government conducted to assess the safety and effectiveness of these devices onboard commercial aircraft? (2) What controls does TSA have in place to help ensure uniform and timely review of air carrier requests to deploy these devices onboard commercial aircraft? The Government Accountability Office (GAO) is recommending that should air carrier interest in deploying these devices resume, TSA should ensure that there is reliable research supporting their use in an aircraft environment and that the agency implement internal controls to govern receipt and review of air carrier requests. The Department of Homeland Security agreed with our recommendations.
Highlights: http://www.gao.gov/highlights/d06475high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−475

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

20. *June 13, Agricultural Research Service* — **Trees resistant to Dutch elm disease.** A large−scale program to screen American elm trees for resistance to Dutch elm disease may lead to trees that can ward off this deadly disease, according to Agricultural Research Service (ARS) scientists and cooperators. The fungus that causes Dutch elm disease (DED) −− Ophiostoma ulmi −− has wiped out around 77 million American elms, since its introduction to the U.S. in 1931. To combat this deadly disease that originated in France, researchers screened thousands of American elm trees for resistance. Thanks to the efforts of ARS scientists and collaborators, enough old specimens were located and kept alive to provide the germplasm necessary to develop DED−tolerant trees.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

21. *June 13, Hamilton Spectator (Canada)* — **Struggling Canadian farmers starved for cash.** New figures from Statistics Canada show the nation's food producers faced a deepening financial crisis last year as their incomes dropped to the lowest levels in three years. By one measure, net farm income fell 7.7 per cent last year to $2.1 billion or eight per cent below the previous five−year average. There's also a squeeze on profit margins −− Statistics Canada's Farm Input Price Index was 134.8 in 2005. That means things farmers need to get crops in the

ground, harvested and shipped that cost $100 in 1992 now cost almost $135. At the same time products that earned $100 in 1997 brought in only $95.40 in March.
Source: http://www.hamiltonspectator.com/NASApp/cs/ContentServer?pagename=hamilton/Layout/Article_Type1&c=Article&cid=1150149010652&call_pageid=1020420665036&col=1112101662835

[Return to top]

Food Sector

22. *June 12, KTOC (Georgia)* — **Canned dog food recalled.** Fifteen kinds of dog food are being voluntarily recalled by Simmons Pet Food, Siloam Springs, AR. Consumer complaints led to the discovery of "random flaking" of the inside coating of the can. The products being recalled include Simmons's Ol Roy, Pot Luck, Twin Pet and American Fare canned dog foods. The dog foods are sold at Wal−Mart and other retail outlets across the country under several private labels.
Source: http://www.wtoctv.com/Global/story.asp?S=5024136&nav=0qq6

[Return to top]

Water Sector

23. *June 13, Associated Press* — **Water improperly tested for lead.** Hundreds of public water systems in North Carolina have been improperly tested for the presence of lead, in part because of poor instructions given out by the state years ago. The faulty testing means some of the systems could have undetected lead problems, but nearly three−fourths of the systems have ignored the state's warnings that they may have been testing the wrong houses. Terry L. Pierce, the director of the Division of Environmental Health, said in April that operators of the systems would have to retest within 30 days. So far, that hasn't happened. Questions about lead testing come as the state's Public Water Supply Section is overwhelmed by the testing requirements of the state's public water systems. Governor Mike Easley has asked for an additional 19 employees for the section. The section sent letters to about 2,650 systems in late March after The News & Observer of Raleigh questioned state officials about systems not testing the houses most likely to have lead−tainted water. The letter said there had been "inconsistent application" of the lead test rules.
Source: http://www.news−record.com/apps/pbcs.dll/article?AID=/20060613/NEWSREC0101/60613006

24. *June 12, U.S. Environmental Protection Agency* — **New Environmental Protection Agency program.** WaterSense, a new water efficiency program launched by the U.S. Environmental Protection Agency (EPA) Monday, June 12, will educate American consumers on making smart water choices that save money and maintain high environmental standards without compromising performance. The WaterSense program aims to raise awareness about the importance of water efficiency, ensure the performance of water−efficient products and provide good consumer information. The WaterSense label will be easily identified on products and services that perform at least 20 percent more efficiently than their less efficient counterparts.

Easily corrected household water leaks frequently rob consumers of eight percent of their water bill. At least 30 percent of water used by household irrigation systems is lost through wind evaporation and improper design, installation or maintenance. The average household adopting water efficient products and practices can save 30,000 gallons per year −− enough to supply a year of drinking water for 150 of their neighbors. Manufacturers can certify these products meet EPA criteria for water efficiency and performance by following testing protocols specific to each product category. In addition, products will be independently tested to ensure EPA specifications are met. These products will be available to families and businesses early next year.
Program information: http://www.epa.gov/watersense/
Source: http://yosemite.epa.gov/opa/admpress.nsf/27166bca9a9490ee852570180055e350/bfb97611364cb2b98525718b0052bb53!OpenDocument

[Return to top]

Public Health Sector

25. *June 13, RIA Novosti (Russia)* — **Ukrainian village put in quarantine over bird flu scare.** Quarantine regulations have been imposed on a village in eastern Ukraine in a bid to deter the spread of bird flu, the Ukrainian emergencies ministry said Tuesday, June 13. Igor Krol, head of the emergencies ministry's press service, said more than 7,000 domestic fowl. He said more than 70 ministry experts were currently working in the area, and that work would be completed within the next two days. Ukraine was previously hit by several bird flu outbreaks in its Crimea region on the Black Sea coast last fall, when more than 150,000 domestic fowl were culled in 40 locations around the peninsula.
Source: http://en.rian.ru/world/20060613/49412879.html

26. *June 13, Agence France−Presse* — **Hong Kong reports suspected human bird flu case in south China.** A 31−year−old man is suspected to have contracted bird flu in southern China. The man is in critical condition in hospital after visiting a wet market in Shenzhen city where live chickens were on sale, the Center for Health Protection said in a statement Tuesday, June 13. It said health department officials from China's Guangdong province had notified Hong Kong of the case. Thousands of people cross the border daily from Guangdong into the southern Chinese territory of Hong Kong.
Source: http://news.yahoo.com/s/afp/20060613/hl_afp/healthfluchinahongkong_060613130528;_ylt=ApTQFe_CWjmdpqaPmEWeAQaJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

[Return to top]

Government Sector

27. *June 13, Associated Press* — **Judge shot in Nevada courthouse; sniper hunted.** A Reno, NV, family court judge was shot and wounded as he stood near a third−floor courthouse window Monday, June 12, and police were looking for man suspected in a slaying across town who had appeared before the judge in a divorce case. Chuck Weller, 53, was hit in the chest around

midday by at least one shot that came through his office window at the Mills B. Lane Justice Center, authorities said. Investigators said Darren Roy Mack, a suspect in a slaying reported later in the day at a Reno apartment building, was a "person of interest" in the shooting at the courthouse. Police also reported that a bomb−sniffing dog had alerted officers to the judge's car in the court's parking garage. A bomb squad was investigating. After the shooting, police closed off six blocks around the courthouse on the edge of Reno's downtown casino district, which otherwise remained open. A SWAT team was called in, and officers conducted a floor−by−floor search of the courthouse and the neighboring parking garages. The attack on Weller "is shocking, but the risk is not shocking. We're well aware this is the inherent risk of trying to solve conflicts, said Darin Conforti, court administrator of Reno Justice Court.
Source: http://www.cnn.com/2006/US/06/12/judge.shot.ap/index.html

[Return to top]

Emergency Services Sector

28. *June 12, Associated Press* — **FEMA stockpiles supplies ahead of Tropical Storm Alberto.** The nation's disaster response agency said Monday, June 12, that evacuation buses and truckloads of food, water and ice were standing by for the year's first big tropical storm −− Tropical Storm Alberto −− but state officials across the Gulf Coast hadn't asked any immediate help from Washington. The Federal Emergency Management Agency (FEMA) did not stockpile supplies for Florida because the state "has indicated that they have the situation well under control," said FEMA spokesperson Aaron Walker. Similarly, the governors of Alabama, Mississippi and Louisiana have not asked for any federal assistance. Additionally, the U.S. Army Corps of Engineers stockpiled tens of thousands of tons of concrete, stone and sandbags to safeguard against any levee breaches around Florida's Lake Okeechobee. FEMA also dispatched 96 truckloads of food, ice and water to holding points in Selma, AL, and Montgomery, AL, ready to go to disaster areas if needed.
Source: http://www.forbes.com/business/energy/feeds/ap/2006/06/12/ap 2810289.html

29. *June 09, New York Times* — **Police department struggles in New Orleans.** Within the New Orleans Police Department, the SWAT team is known as The Final Option. Before Hurricane Katrina, it was assigned to the city's worst crimes. But the team is running dangerously low on firepower. Flooding ruined 300 of its guns, its bullet−resistant shields and the bulk of its ammunition, none of which have been replaced more than nine months after the hurricane. The 40−man team has had to borrow body armor from suburban forces, and the Police Department is lining up corporate sponsors to contribute more. The SWAT unit's difficulties reflect how far from normal many police operations remain in New Orleans, as residents return and another hurricane season begins. Like the rest of the city, the police force is still struggling to recover from the calamity of Hurricane Katrina, which knocked out its headquarters, overwhelmed its ability to maintain control and prompted desertions that tarnished the force's reputation. More than 200 officers deserted during the storm and were fired or suspended. Many veteran officers retired, and some of the youngest officers quit and left town. As a result, the size of the force has dropped to about 1,400 officers on the street, from nearly 1,700 before the hurricane.
Source: http://www.nytimes.com/2006/06/13/us/13orleans.html?_r=1&hp&ex=1150171200&en=4e9019d5a2e0a39b&ei=5094&partner=homepage&o ref=slogin

30. *June 01, Federal Highway Administration* — **Departments of Homeland Security and Transportation release review of gulf state's mass evacuation plans.** Congress requested the Department of Transportation, in cooperation with the Department of Homeland Security, to "review and assess Federal and State evacuation plans (including the costs of the plans) for catastrophic hurricanes and other catastrophic events impacting the Gulf Coast region and report its findings and recommendations to Congress." This assessment included: (1) all safe and practical modes of transportation available for evacuations; (2) the extent to which evacuation plans are coordinated with neighboring States and adjoining jurisdictions; (3) methods of communicating evacuation plans and preparing citizens in advance of evacuations; (4) methods of coordinating communication with evacuees during plan execution; (5) the availability of food, water, restrooms, fueling stations, and shelter opportunities along the evacuation routes; (6) the time required to evacuate under the plan; and (7) the physical and mental strains associated with the evacuation. The assessment also includes issues and lessons learned from evacuations associated with Hurricanes Katrina and Rita and other recent hurricanes.
Report: http://www.fhwa.dot.gov/reports/hurricanevacuation/rtc_chep_eval.pdf
Source: http://www.fhwa.dot.gov/reports/hurricanevacuation/index.htm

[Return to top]

Information Technology and Telecommunications Sector

31. *June 12, Security Focus* — **Symantec Antivirus remote stack buffer overflow vulnerability.** Multiple Symantec products are susceptible to a remote stack buffer overflow vulnerability.
Analysis: This issue allows remote attackers to execute arbitrary machine code with SYSTEM level privileges, facilitating the complete compromise of affected computers.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/18107/info
Solution: Symantec has released an advisory with further information regarding this issue. Fixes are available at: http://www.symantec.com/techsupp/enterprise/select_product_updates.html
Source: http://www.securityfocus.com/bid/18107/references

32. *June 12, Security Focus* — **Mozilla Firefox, SeaMonkey, and Thunderbird multiple remote vulnerabilities.** The Mozilla Foundation has released thirteen security advisories specifying security vulnerabilities in Mozilla Firefox, SeaMonkey, and Thunderbird. Analysis: These vulnerabilities allow attackers to execute arbitrary machine code in the context of the vulnerable application and crash affected applications. While running JavaScript code with elevated privileges it may potentially allow the remote execution of machine code and gain access to potentially sensitive information.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/18228/info
Solution: New versions of Firefox, SeaMonkey, and Thunderbird are available to address these issues. Most Mozilla applications have self−updating features that may be used to download and install fixes. For information on obtaining and applying fixes: http://www.securityfocus.com/bid/18228/references
Source: http://www.securityfocus.com/bid/18228/discuss

33.

June 12, Register (UK) — **Taiwan fingered as the hub of spam distribution.** Sixty−four percent of servers controlling spam traffic are located in Taiwan, according to a survey by e−mail security firm CipherTrust. The U.S. accounts for 23 percent of the machines identified on CipherTrust's spam server blacklist with China in a fairly distant third place (three percent). CipherTrust obtained its figures after deploying a network of zombie−like machines across the world to gather intelligence on spamming operations.
Source: http://www.theregister.co.uk/2006/06/12/spam_distribution_st udy_ciphertrust/

34. *June 12, IDG News Service* — **Yahoo e−mail under worm attack.** A mass−mail worm that exploits a vulnerability in Yahoo's Web e−mail is making the rounds but the impact appears to be low, security vendor Symantec said Monday, June 12. The worm, which Symantec calls JS.Yamanner@m, is different from others in that a user merely has to open the e−mail to cause it to run, said Kevin Hogan, senior manager for Symantec Security Response. The worm, written in JavaScript, takes advantage of a vulnerability that allows scripts embedded in HTML e−mail to run in the users' browsers.
For more information on this: http://us.mcafee.com/virusInfo/default.asp?id=description&vi rus_k=139913
Source: http://www.infoworld.com/article/06/06/12/79193_HNyahooworma ttack_1.html?source=rss&url=http://www.infoworld.com/article /06/06/12/79193_HNyahoowormattack_1.html

35. *June 12, CNET News* — **Craigslist suffers third outage in a week.** Craigslist.org, one of the Web's top classified sites, suffered its third outage in the last week on Monday, June 12. An unidentified glitch prevented many visitors to Craigslist from accessing the site for about an hour, said Jim Buckmaster, the company's chief executive. Craigslist went down twice last week and the company's technicians suspect all three outages are related, Buckmaster said. Craigslist is the seventh most popular site on the Internet in terms of page views.
Source: http://news.com.com/Craigslist+suffers+third+outage+in+a+wee k/2100−1038_3−6083034.html?tag=nefd.top

36. *June 12, Federal Computer Week* — **DoD toughens up wireless LAN security rules.** The Department of Defense (DoD) has tightened policies on the use of wireless local−area networks (WLANs), in a memo released earlier this month, which requires beefed up encryption and security since the last DoD wireless policy memo was released in April 2004. The new policy also requires all 802.11a, b and g DoD WLAN systems to be equipped with an around−the−clock intrusion detection system that can geo−locate hackers or operators of rogue access points. The new DoD WLAN policy, signed by the assistant secretary of Defense for networks and information integration Friday, June 2, states that any WLAN products connected to the DoD Global Information Grid must be certified and validated for secure end−to−end communications and interoperability.
Source: http://www.fcw.com/article94870−06−12−06−Web

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of a buffer overflow vulnerability in Symantec Client Security and Symantec Antivirus Corporate Edition. Successful exploitation may allow a remote, unauthenticated attacker to execute arbitrary code with SYSTEM privileges. We are not aware of any public exploits at this time. For more information please review the following:

VU#404910 − Symantec products vulnerable to buffer overflow:
http://www.kb.cert.org/vuls/id/4049100

Symantec Advisory SYM06−010 − Symantec Client Security and Symantec AntiVirus Elevation of Privilege:
http://securityresponse.symantec.com/avcenter/security/Conte nt/2006.05.25.htmll

US−CERT will advise as more information becomes available.

Active Exploitation of a Vulnerability in Microsoft Word

US−CERT is aware of an increase in activity attempting to exploit a vulnerability in Microsoft Word. The exploit is disguised as an email attachment containing a Microsoft Word document. When the document is opened, malicious code is installed on the user's machine. More information about the reported vulnerability can be found in the following:

TRA06−139A − Microsoft Word Vulnerability:
http://www.us−cert.gov/cas/techalerts/TA06−139A.htmll

VU#446012 − Microsoft Word buffer overflow:
http://www.kb.cert.org/vuls/id/446012

Review the workarounds described in Microsoft Security Advisory 919637:
http://www.microsoft.com/technet/security/advisory/919637.ms px

US−CERT strongly encourages users not to open unfamiliar or unexpected email attachments, even if sent by a known and trusted source. US−CERT will continue to update current activity as more information becomes available.

PHISHING SCAMS

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT. http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 38566 (−−−), 6881 (bittorrent), 4672 (eMule), 445 (microsoft−ds), 25 (smtp), 135 (epmap), 139 (netbios−ssn), 80 (www), 113 (auth) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

37. *June 12, Boise State Radio (ID)* — **High water threatens North Idaho levees.** Farmers in North Idaho are fearing the worst from rising waters in the Kootenai River. The governor has already declared a state of emergency for the town of Bonners Ferry. Now all eyes are on the weather forecast. First came a heat wave in May that caused rapid snowmelt. Then days of heavy rain. All the extra water prompted the U.S. Army Corps of Engineers to increase spills at Libby Dam in Montana. . It adds up to what is now a surge of high water in Idaho's Kootenai River Basin. The swollen river is licking away at levees that hold back the waters in this former lakebed. Some farms have already flooded, causing millions of dollars' worth of crop damage. An emergency team is dumping fresh rock to stabilize the dike before an expected onslaught of more heavy rain this week. With the river just a foot or so below flood stage, teams of local volunteers with sandbags are standing by.
Source: http://www.nwpr.org/HomepageArticles/Article.aspx?n=1949

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer